

Re: SP2/firewall

Source: <http://www.derkeiler.com/Newsgroups/alt.computer.security/2005-01/0633.html>

From: winged (winged_at_nofollow.com)

Date: 01/22/05

Date: 22 Jan 2005 17:03:03 EST

ROBERT S AMP BA Drake wrote:

> *Run a scan on your system with the MS SP2 firewall on. It has more holes than swiss cheese.*

>

> *"JOHANNA NORDMYR" <j.nordmyr@tele2.se> wrote in message news:7KfId.15699\$Of5.10827@nntpserver.swip.net...*

>

>>*I've just recently installed the SP2 and decided to use the firewall included, instead of Norton's. As far as I can tell it seems to be working okay, but some of the icons are giving me a headache... At some websites "integrety report" pops up. Why??*

>>

>

>

>

You can control, very specifically, very manually all communication that the SP2 Firewall is allowed. The control panel applet under the exception tab allows constraint by program and port. I am not sure why the applet portion of the system deems I need remote desktop, remote assistance and UPNP exposed to the world (by default) nor why they insist I expose ping replies. I have gone to some efforts just to ensure those very services were not exposed.

If you were using (for example) SP2 Firewall, under the exceptions tab, you could restrict the ports and the addresses your e-mail client was allowed to view. Doing this breaks over the web viewing functionality (this is also the "behavior" of my e-mail client (Thunderbird)) but for me, this is not a bad thing as it also breaks many compromise scenarios (I don't allow scripting in mail)(OK I am retentive). Additionally one "can" control the XP Firewall via a rule file.

This is how one can manage a network of XP firewalled computers. By regulating the firewall rules you can control the network user permissions. This is easily managed both dynamically via SMS or similar central management tool, or via bootup login script. The rules are refreshed on bootup by specifically and dynamically concatenating the rule file. For example you "can" have certain blocks (port or address) that you wish to apply across a domain, concatenating rules that apply

alt.computer.security: Re: SP2/firewall

to a specific user. But this finite level of control you can enforce is somewhat of a pain to manage for a home network.

The firewall can be competent. If you use the SP2 firewall, Ensure you check the default sett